A Atividade de Inteligência Brasileira: Papel, Perfil e Perspectivas

Diana dos Santos Benites[1]
Henrique Berbigier Omegna de Souza[2]
Marianna de Oliveira Rodrigues[3]
Victor Domingues Ventura Pires[4]
William Ribeiro Marafon[5]

Orientador: *Prof. Me. Naiane Inez Cossul*[6]

RESUMO

Este artigo tem como proposta uma análise acerca das atividades de inteligência no Sistema Internacional, de modo a apresentar sua relevância no campo estratégico, quanto à formulação de políticas nos campos de Segurança e Defesa dos Estados e, principalmente, do Brasil. Partindo deste ponto, objetiva-se, a partir da revisão histórico-bibliográfica, legitimar o papel das atividades de inteligência em nível internacional, no que se refere à defesa e à projeção do poder do Estado, e compreender esta formulação a nível nacional. Este estará seccionado da seguinte maneira: primeiramente, far-se-á a observação do panorama, atual e histórico, das atividades de inteligência na esfera internacional, passando de forma sucinta pelas definições clássicas. Logo, apresentar-se-á o histórico das atividades de inteligência no Brasil, objetivando expor a forma pela qual deu-se a evolução desta temática no cerne do Estado brasileiro. Por fim, serão apresentados os objetivos, desafios e oportunidades abordados na Estratégia Nacional de Inteligência, a fim de mapear o caminho até a consolidação da atuação da inteligência como parte fundamental dos arranjos de Defesa e Segurança do Brasil.

Palavras-chave: Inteligência, Segurança, Defesa, Brasil, Desafios Estratégicos

INTRODUÇÃO

A Segurança do Estado, conforme definido por Maquiavel (1532), trata-se de um mecanismo fundamental para a garantia da integridade estatal, dos interesses nacionais e da salvaguarda da soberania. Embora ao longo dos anos tenha havido o remodelamento e até mesmo a expansão de tais conceitos, levando-os para além do nível físico-militar, para o campo socioeconômico, a percepção que se tem acerca da importância da Segurança ainda é a mesma. Desta forma, desenvolveram-se uma série de ferramentas que objetivam facilitar a execução dos interesses securitários do aparato estatal, e, dentre estas, estão as atividades de Inteligência, como um elemento central para o alcance completo dos objetivos do Estado e para o aumento da projeção do poder político, econômico, militar e tecnológico.

[1]Graduanda do 3º semestre de Relações Internacionais do Centro Universitário Ritter dos Reis (UniRitter) - dianasbenites13@gmail.com
[2]Graduando do 7º semestre de Relações Internacionais do Centro Universitário Ritter dos Reis (UniRitter) - henriqueb.omegna@gmail.com
[3]Graduanda do 7º semestre de Relações Internacionais do Centro Universitário Ritter dos Reis (UniRitter) - marianna.oliveira08@gmail.com
[4]Graduando do 5º semestre de Relações Internacionais do Centro Universitário Ritter dos Reis (UniRitter) - victordventurap@gmail.com
[5]Graduando do 7º semestre de Relações Internacionais do Centro Universitário Ritter dos Reis (UniRitter) - william_rm1@hotmail.com
[6]Professora de Relações Internacionais no Centro Universitário Ritter dos Reis (UniRitter). Doutoranda em Estudos Estratégicos Internacionais (PPGEEI-UFRGS). Mestre e Graduada em Relações Internacionais (UFSC) - naiane.cossul@uniritter.edu.br

Apesar de sua fundamental relevância durante os períodos de guerra, logo após a Guerra Fria, quando as tensões se acalmaram no meio internacional, as atividades de Inteligência passaram a ser deixadas de lado, sob a premissa de que sua necessidade havia caído em desuso. Entretanto, claramente a Inteligência continuava a ter essencial importância, uma vez que, foi neste período que se intensificaram as instabilidades internacionais, ainda como heranças das grandes guerras e como consequências do início do processo de globalização pela qual o Sistema Internacional passava, que exigiam demandas cada vez maiores e mais diversificadas de informações com a finalidade de prever e prevenir ataques que pudessem ferir a integridade, os interesses e a soberania estatal, reiterando a necessidade latente do estabelecimento de sistemas de inteligência nacionais dado o amplo leque de ameaças com que se trabalha no período contemporâneo, cujo exige uma maior diversificação de operações e aplicações das atividades de inteligência estratégica.

Diante dessa realidade, o atual artigo visa demonstrar o desenvolvimento histórico e a aplicação atual das atividades de inteligência a partir de uma ótica nacional, mas também atento ao cenário externo, almejando contribuir para os estudos de defesa e possibilitar uma melhor compreensão da estratégia brasileira de defesa e inteligência e sua crescente coesão, tal qual do modus operandi de nosso sistema nacional de inteligência, o qual tem dado passos importantes em direção à segurança e garantia dos objetivos e interesses nacionais em anos recentes.

1. O SURGIMENTO DO CONCEITO DE INTELIGÊNCIA E SUA RELEVÂNCIA COMO MECANISMO DE TOMADA DE DECISÃO

A inteligência, fora do campo que se refere às capacidades cognitivas, pode ser definida como qualquer conjunto de informações coletadas, organizadas e analisadas, de modo a atender às demandas e necessidades de um tomador de decisões. Dentro da ciência da informação, a inteligência trata-se especificamente da parte que se refere à agregação, análise e tratamento minuciosos em uma pirâmide informacional, que se forma a partir das várias fases pelas quais as informações passam, desde sua forma bruta, até chegar à sua fase final, na qual são utilizadas para auxiliar na tomada de decisões dos mais variados atores, desde governos, empresas, ou até mesmo organizações de caráter social (CEPIK, 2003).

Contudo, dentro do âmbito da segurança estratégica, a definição do termo inteligência acaba sendo um pouco mais específica e restrita aos fluxos informacionais estruturados na coleta de informações, das mais variadas fontes – indivíduos, sinais eletromagnéticos, imagens, interceptação de linhas telefônicas, etc. – sem a presença de consentimento e/ou colaboração daqueles cujos são alvos de tais práticas. Ou seja, no campo securitário, de modo geral, a inteligência tem significado equivalente à extração de dados secretos, a fim de auxiliar os Estados a prever e dissuadir possíveis ataques que possam ameaçar sua soberania. Ainda dentro do âmbito da segurança internacional, Marco Cepik, em seu livro *Espionagem e Democracia*, afirma que:

> Serviços de inteligência são agências governamentais responsáveis pela coleta, pela análise e pela disseminação de informações consideradas relevantes para o processo de tomada de decisões e de implementação de políticas públicas nas áreas de política externa, defesa nacional e provimento de ordem pública. Essas agências governamentais também são conhecidas como serviços secretos ou serviços de informação (CEPIK, 2003, p. 13).

Deste modo, é pertinente avaliar a temática da inteligência sob uma ótica mais ampla do que apenas como um e apoio à tomada de decisão. Trata-se de um braço dos governos, fortemente aliado à formulação de suas políticas e estratégias de defesa e segurança, bem como aos órgãos responsáveis por sua execução, como as Forças Armadas, as polícias e a diplomacia, formando assim o núcleo coercitivo do Estado moderno (CEPIK, 2003).

Diante do exposto, a inteligência se configura como elemento central para que se atinja os objetivos defensivos do Estado. Assim, considerando-se que um sistema de inteligência

adaptado aos cenários de ameaças difusas é uma das condições estruturantes para o desenvolvimento de capacidades defensivas de um país no Sistema Internacional, este trabalho enquadra-se nas perspectivas teórico-conceituais da obra realista de Robert Gilpin (1981), segundo a qual o poder refere-se às capacidades políticas, econômicas, militares e tecnológicas dos Estados. Nesse sentido, a atividade de inteligência configura-se como um projeto estratégico para o Estado.

A presença da atividade de inteligência nas relações entre os Estados é mais antiga do que se pode presumir. Seu uso remonta à antiguidade – adotada já pelos Estados absolutistas europeus no século XVI (CEPIK, 2003) - para descobrir quais eram os planos de seu inimigo, de modo a antecipar suas estratégias de defesa. Entretanto, seu surgimento, enquanto matéria de estudo no campo de Defesa e Segurança, se dá no século XX, logo após a Primeira Guerra Mundial com a implementação do Tratado de Versalhes, no qual imperavam os princípios de manutenção da paz de da segurança, sendo ratificada a partir do Tratado de *Briand Kellogg*, no qual os Estados concordam que a guerra não pode mais ser empregada como um instrumento de Política Externa e de afirmação do poder (SEITENFUS, 2003). Assim, com a nova organização da sociedade pós-guerra, a atividade de inteligência ganhou uma nova escala operacional, sendo agora classificada como uma função social organizada, de cunho profissional e permanente, de caráter essencial para a governabilidade e salvaguarda da segurança do Estado, não apenas nos momentos de guerra, mas também durante os períodos de paz e ordem institucional (GONÇALVES, 2003).

Sua finalidade principal resulta do conjunto de prioridades que cada Estado leva em conta na formulação de sua Política Externa, legando às agências de inteligência a missão de obter, lapidar e ordenar dados que possam fornecer o suporte necessário para o alcance dos objetivos nacionais, seja na área de defesa ou na identificação de oportunidades. Entretanto, a atividade de inteligência pode se ocupar também com questões atreladas ao âmbito interno do país, cumprindo as funções de proteção do Estado enquanto ator, assim como da sociedade e da garantia de estabilidade das instituições democráticas e da gestão pública (ABIN, 2018d). Suas áreas de atuação ainda podem se dividir entre os campos i) estratégico - que tange à formulação de políticas públicas e instrumentos legais; ii) tático - atrelado ao planejamento de ações militares e policiais; ou ainda, iii) operacional - que se refere ao apoio nas ações efetivas de combate militar e prevenção de ações ilegais (ABIN, 2018d).

Ainda que bastante antiga, a atividade de inteligência só ganhou caráter institucionalizado (ganhando estabilidade e valor frente à administração do Estado) a partir do século XX, e até quase seu final ainda se acreditava que este tipo de atividade era apenas um subproduto das guerras, de necessidade passageira, e que com o final dos conflitos entraria em desuso (CEPIK, 2003). Ao final da Guerra Fria, por exemplo, os serviços de inteligência de vários países tiveram seus orçamentos significativamente reduzidos, uma vez que os governos acreditavam não haver necessidade para continuar investindo em seu funcionamento, já que as guerras haviam findado.

Por outro lado, era justamente neste momento que o Sistema Internacional se tornava mais instável, dado o legado das grandes guerras do século XX, e as consequências do processo de globalização pelo qual o mundo passava. Isso tornava as demandas por informação mais exigentes e diversificadas, a fim de que se pudesse prever e prevenir possíveis ataques que tivessem como objetivo a desestabilização de um Estado que, nesta conjuntura, traria impactos a todo o sistema, em maior ou menor grau. Tirando proveito desta necessidade, surgiram nesta época muitas tecnologias informacionais, que deram origem também a uma série de empresas de caráter privado que ofereciam serviços de informação, com a promessa de auxiliar na defesa dos países, competindo com as próprias agências nacionais de inteligência pela atenção e investimentos do governo.

1.1. Uso da inteligência durante as guerras

A atividade de inteligência foi fortemente utilizada nos períodos de guerras e conflitos, desde a Idade Média, quando Maomé se fez valer de agentes infiltrados em Meca (em 624) para impedir avanço de soldados árabes à Medina (ARAÚJO, 2005). Há registros referentes a estas atividades que remontam ao Velho Testamento da Bíblia, ou seja, antes mesmo da formação dos Estados *westphalianos* europeus no século XVII. No período do Renascimento, desenvolveu-se tal atividade com o objetivo de obtenção de informações e comunicações destas, principalmente no que dizia respeito aos inimigos (CEPIK, 2003).

No Manual da Arte da Guerra de Sun Tzu, já haviam referências nesse sentido, pois, para ele, conforme Cepik (2003, p. 87), "o reconhecimento do campo de batalha e do inimigo sempre foi considerado um elemento essencial da capacidade de comando do general". A Revolução Francesa e Napoleão Bonaparte modificaram e transformaram o significado de inteligência para o sentido de comando. Napoleão organizava seu quartel general em unidades distintas e independentes, tendo uma unidade específica para o controle da inteligência, e mantendo-a em segredo, às vezes até mesmo do imperador (CEPIK, 2003).

Após a Revolução Gloriosa, as redes de inteligência que haviam sido formadas se mantiveram, evidenciando a necessidade dessas atividades à afirmação da autoridade do Estado Nacional (CEPIK, 2003). Já na Guerra de Secessão, a Inteligência inovou em suas ações utilizando-se de códigos, cifras, reconhecimento aéreo efetuado por balões e fotografias, nas quais eram inseridas mensagens (microfilmagem) (ARAÚJO, 2005).

Outra modernização na atividade de Inteligência pode ser percebida durante a Primeira Guerra Mundial, em que passou a se usar tecnologias e artifícios não efetuados pelo homem. E após a Primeira Guerra Mundial, no período entre guerras, os primeiros órgãos de inteligência se institucionalizaram. Na Segunda Guerra Mundial, grandes potências como Alemanha e Japão, possuíam serviços de inteligência instalados pelo mundo, como é o exemplo da Polícia Militar Secreta Japonesa, *Kempei Tai*, que havia logrado infiltrar um espião meses antes do ataque de *Pearl Harbour* (ARAÚJO, 2005).

Ainda referente a Segunda Guerra Mundial, os Aliados também utilizaram amplamente seus serviços de inteligência, enviando agentes a outros territórios para organizar grupos de resistência, por exemplo. E ao término do conflito, descobriu-se que os países utilizavam estes serviços contra os próprios aliados, basicamente por meio da espionagem. Na Guerra Fria, as agências como a CIA *(Central Intelligence Agency)* e NSA *(National Security Agency)* elaboravam relatórios nos quais as decisões políticas norte-americanas eram baseadas. A KGB (Comitê de Segurança do Estado da URSS) combinava operações secretas e atividades de uma Polícia Federal. Neste período, o grande desenvolvimento tecnológico contribuiu para o mais eficiente monitoramento mútuo das potências (ARAÚJO, 2005).

Os Serviços de Inteligência tiveram participação - por meio da obtenção e análise de informações, infiltrações de agentes e missões clandestinas e outras vezes propagando ideais dos governos aos quais pertenciam, agindo como uma espécie de aparato de relações públicas no exterior - em momentos marcantes da história, tais como a queda do muro de Berlim em 1989 (KGB), o insucesso do golpe contra Gorbatchev em 1991 (KGB), a Revolução dos Aiatolás no Irã em 1979 (CIA), a invasão do Kuwait pelo Iraque em 1990 (CIA), a Guerra do Yom Kippur em 1973 (Mossad – Israel) (ARAÚJO, 2005). Apesar disso, a cooperação da inteligência é um efetivo instrumento para desenvolver as relações internacionais (RIBEIRO, 2006), sendo definida como "a única maneira conhecida de reduzir as incertezas" (DUROSSELLE, 2000, p. 117).

1.2. Aplicação da inteligência nos dias atuais: uso como mecanismo atrelado à estratégia de defesa

Quando se aborda as atividades de inteligência no período hodierno, é necessário ater-se ao fato de que os sistemas nacionais de inteligência, e principalmente as organizações

originadas por estes, possuem um leque muito mais amplo de operações do que seus antecessores históricos. Nas últimas décadas os serviços de inteligência diversificaram o escopo de suas aplicações de tal forma que passaram a abranger atividades de contra inteligência, antiterrorismo, combate ao crime organizado, narcotráfico e crimes eletrônicos, culminando em uma variedade mais complexa de empreendimentos (CEPIK, 2003).

Essa complexidade é um fato tão inerente aos sistemas nacionais de inteligência que, em seu último período presidindo o Comitê de Inteligência do Senado dos EUA, o senador Richard Shelby recomendou que, em ordem de combater os desafios do século XXI, "pensássemos o impensável" (SENATOR, 2001). Esse conselho jamais poderia ter sido tão pontual, pois tal pronunciamento, feito em 18 de maio de 2001, prescinde o atentado de 11 de setembro do mesmo ano, quando fundamentalistas islâmicos radicais da Al Qaeda fazem o impensável, realizando um ataque aéreo suicida ao território dos Estados Unidos com aviões sequestrados em pleno voo.

O ataque às torres gêmeas foi um marco para a ordem internacional, assim como o foi para a aplicação estratégica de inteligência, pois "o que pode ser estratégico está intimamente ligado à nova ordem internacional, [...] após o 11 de setembro, o mundo viu uma nova direção estratégica, voltada para a defesa militar em relação ao terrorismo" (RIBEIRO, 2006, p. 118). Consequentemente, o terrorismo internacional e sua tática de combate assimétrico tem se provado uma ameaça não apenas à ordem internacional como também aos vários sistemas de inteligência nacionais que a compõe.

Os serviços de inteligência nacionais, embora tenham que enfrentar inúmeras adversidades no cenário contemporâneo, ainda agem instigados pela atuação do Estado diante das,

> questões estratégicas de sua sociedade, com objetivos claros de posição e inserção internacional, e ao mesmo tempo na construção de um parâmetro de segurança de Estado, além de defesa contra ameaças externas, mas a atividade é ampliada no contexto exterior em função de coleta de informações para construção de cenários competitivos de participação do Estado, em relação ao mercado externo, sua posição e percepção de valor, imagem sólida e concreta de estabilidade, e de posicionamento de sua soberania perante as grandes potências, além da relação diplomática e propagandista do Estado perante os organismos internacionais. (RIBEIRO, 2006, p. 114).

Dentre os desafios do século atual acentuados no discurso do Senador Shelby (SENATOR, 2001), residem os avanços tecnológicos, a velocidade com que ocorre a disseminação de informação e os obstáculos para se atingir uma cooperação entre agências nacionais de inteligência sem que o Estado se coloque em uma posição vulnerável às atividades de espionagem[7] ou roubo de tecnologias. Diante disso, muitos paradoxos são levantados quanto ao emprego das atividades de inteligência no século XXI, tanto na cooperação entre agências de inteligência de nações diferentes quanto na imagem que essas agências refletem para suas respectivas sociedades em questão da transparência demandada das instituições contemporâneas (CEPIK, 2003).

Atualmente, no entanto, as agências de inteligência têm sido mais abertas quanto às suas atividades oficiais, um fator paradoxal visto que a atividade de inteligência requer um certo nível de sigilo e discrição. Não para tanto, essa abertura desperta a discussão dos limites ao alcance destas atividades visando a preservação da privacidade individual de cada cidadão, pois

---

[7]Um dos mais notórios exemplos, em âmbito nacional, foi a descoberta da espionagem estadunidense voltada à ex-presidente Dilma Rousseff e à Petrobrás por telefonemas e e-mails, e, em âmbito internacional, a criação e propagação do *Wikileaks*, site criado por Julian Assange para divulgar segredos estatais. Por fim, o caso de Edward Snowden ajuda a ilustrar o perigo que as agências de inteligência estão sujeitas até mesmo no que tange seu ambiente interno e o controle e supervisão de seus colaboradores (EDWARD..., 2016).

com o suporte das leis e do Estado, as agências de inteligência têm capacidade para vigiar e interferir em comunicações alheias[8] (SHANE, 2016).

2. EVOLUÇÃO HISTÓRICA DAS ATIVIDADES DE INTELIGÊNCIA NO BRASIL

A atividade de inteligência no Brasil, sendo entendida como a função exercida por uma instituição, é algo recente, logo, qualquer discussão que se proponha a apresentar ou debruçar-se sobre um estudo analítico ou crítico necessariamente precisa desenvolver os mecanismos e fatos históricos que levaram a atual conjuntura da inteligência nacional. Desta forma, a presente seção propõe-se a apresentar uma revisão histórica do desenvolvimento dos aparatos de inteligência atrelados à Defesa Nacional, com o objetivo de utilizar-se da base histórica nacional para o embasamento das análises a serem discutidas neste trabalho.

2.1. Introdução à Inteligência e Defesa Brasileira

Tem-se através da retenção e proteção da informação, um dos bens mais preciosos e estratégicos na composição dos Estados modernos. Atualmente a disponibilidade de tecnologias e estratégias de proteção da informação viabilizam a tomada de decisão por parte dos agentes estatais, através do processamento de dados, de informações e de conhecimentos. Entretanto, tamanha complexidade de defesa e inteligência surgiu através de processos contínuos ao longo da história brasileira. A cronologia de criação dos órgãos de inteligência do Brasil passou por quatro fases distintas: i) embrionária de 1927 a 1964; ii) da bipolaridade de 1964 a 1990; iii) de transição de 1990 a 1999 e iv) contemporânea de 1999 aos dias atuais.

A fase embrionária teve início em 1927, no governo de Washington Luís, que foi responsável pela criação do Conselho de Defesa Nacional (CDN). Sua continuidade foi dada no governo de Getúlio Vargas, que vigorou entre 1930 e 1945. Durante o governo Vargas foram criados o Conselho Superior de Segurança Nacional (CSSN) e o Conselho de Segurança Nacional (CSN), que mantiveram a ordem administrativa até a criação do Serviço Federal de Informações e Contrainformações (SFICI) em 1946, que seguiu suas atividades até 1964. Nesta fase a atividade estava inserida, de forma complementar, nestes conselhos de governo, que, em suas respectivas épocas, gerenciavam a inteligência nacional. A importância desta fase reside na construção das primeiras estruturas governamentais voltadas para a análise de dados e para a produção de conhecimentos (ABIN, 2018c).

De forma mais apurada, o CDN, instituído no governo Washington Luís, entrou em vigor em 1927 através do decreto nº 17.999 de 29 de dezembro. Sendo composto primariamente pelo Presidente da República, inúmeros ministros, além do Chefe do Estado Maior do Exército e da Marinha. Tornou-se o Conselho de mais alto nível de assessoramento ao Presidente da República vigente, contendo e formalizando a execução das políticas de defesa e segurança nacional. Como mencionado, a função primária do CDN era garantir a assessoria direta ao Presidente da República em situações de guerras e ameaças à paz e a ordem nacional, tendo um caráter mais objetivo e relacionado à manutenção do Estado democrático brasileiro e de sua soberania nacional.

Com o passar do tempo sua função e importância cresceram exponencialmente, abordando novos assuntos relacionados à segurança e à manutenção da ordem, tornando possível a criação do Conselho Superior de Segurança Nacional, já no governo de Getúlio Vargas, em 1934. O CSSN duraria até o governo Dutra, que, diante do contexto pós Segunda Guerra Mundial e da deflagração da Guerra Fria e do mundo bipolar, viu a necessidade de uma nova conceituação para a inteligência brasileira, criando o SFICI, que, em seu primeiro momento serviu como formador de conceitos e de marcos para regular as atividades de inteligência, tendo assumido, a partir do governo de Juscelino Kubitschek, em 1958, o papel

[8] Utilizando-se do exemplo apresentado pela notícia, podemos referenciar a manipulação indireta de resultados através do direcionamento de um discurso, como parte de uma política oficial de inteligência (SHANE, 2017).

central como entidade de inteligência nacional, sendo considerado o primeiro órgão de inteligência brasileiro (ABIN, 2018c).

A fase da bipolaridade é marcada pela ascensão do Regime Civil-Militar, e onde temos a criação do Serviço Nacional de Informações (SNI) em 1964. O passo inicial para sua criação foi dado pelo Presidente Castelo Branco, passando pelos demais presidentes do Regime que o sucederam, até seu fim, em 1990, no governo de José Sarney. Nesta época, em particular na história brasileira, temos a emersão de um novo pensamento: o alinhamento com a agenda norte-americana, que proporcionou novas diretrizes e estratégias para o SNI (ABIN, 2018c).

Com a redemocratização e o fim do bipolarismo, que se deu pela queda do bloco comunista, em 1991, a atividade de inteligência passou por um importante processo de reavaliação para se adequar aos novos contextos governamentais e geopolíticos. A Inteligência tornou-se vinculada à Secretaria da Presidência da República, primeiro como Departamento de Inteligência (DI) e, posteriormente, como Subsecretaria de Inteligência (SSI) (ABIN, 2018c).

Com o revisionismo das estratégias de defesa, temos o início da nova fase, conhecida como fase de transição, tendo seu início em 1990 e durando até 1999. Sendo iniciada pelo Presidente Fernando Collor de Mello, responsável pela criação da Secretaria de Assuntos Estratégicos (SAE) e pela inserção da Secretaria Geral da Presidência da República (SGPR) como parte da estrutura da inteligência nacional. O marco final desta fase é dado pela criação da Casa Militar da Presidência da República (CMPR), em 1996, que assumiu as responsabilidades do SGPR, e que durou até 1999, sob o governo de Fernando Henrique Cardoso (ABIN, 2018c).

2.2. A inteligência sob a égide do SISBIN

A fase contemporânea inicia-se com a criação do Sistema Brasileiro de Inteligência (SISBIN) e de seus órgãos subordinados, que foi concomitante à grande reforma na área da Defesa realizada pelo governo Fernando Henrique, em 1999, onde as Forças Armadas passaram a estar sob a gerência do Ministério da Defesa, controlado por um civil (LIMA, 2012). O SISBIN tem sua definição dada pelo Art. 1º da lei Nº. 9.883, de 7 de dezembro de 1999, onde "fica instituído o Sistema Brasileiro de Inteligência, que integra as ações de planejamento e execução das atividades de inteligência do País, com a finalidade de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional" (BRASIL, 1999), sendo baseado nos fundamentos referenciados pelo parágrafo 1º da mesma lei como,

> [...] a preservação da soberania nacional, a defesa do Estado Democrático de Direito e a dignidade da pessoa humana, devendo ainda cumprir e preservar os direitos e garantias individuais e demais dispositivos da Constituição Federal, os tratados, convenções, acordos e ajustes internacionais em que a República Federativa do Brasil seja parte ou signatário, e a legislação ordinária (BRASIL, 1999).

Como parte essencial do SISBIN, o mais importante órgão para a gestão e ação da inteligência nacional foi criado: a Agência Brasileira de Inteligência (ABIN), como executor da atividade de inteligência brasileira, tendo suas atribuições definidas pelo Art. 3º da mesma lei de criação do SISBIN[9], sendo o "órgão central do Sistema Brasileiro de Inteligência, terá a seu cargo planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País, obedecidas à política e às diretrizes superiormente traçadas nos termos desta Lei" (BRASIL, 1999). Todavia, a ABIN, por promessa do próprio FHC, deveria permanecer sob contato e supervisão direta do Presidente da República, todavia, através da Medida Provisória Nº. 1.994-4, de 13 de janeiro de 2000, colocou-se a agência sob mando e também como "conexão" entre a Presidência e o órgão, o Gabinete de Segurança Institucional da Presidência

[9] Definição que foi revista pela Medida Provisória Nº 2.216-37, de 31 de agosto de 2001, e que é apresentada no texto (BRASIL, 2001).

da República (GSI/PR)[10], que substituiu a Casa Militar; estando a ABIN, a partir de então, subordinada ao Ministro-Chefe do GSI/PR (BRASIL, 2001).

Ainda na mesma lei de sua criação, como forma de centrar e guiar as atividades executadas pela ABIN, em seu Art. 2º nos é ofertada a definição de inteligência, como sendo "a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado" (BRASIL, 1999). E, como ressalta Lima (2012), não se pode confundir as atividades desenvolvidas pela ABIN como aquelas desenvolvidas pelos castrenses, a primeira, é uma inteligência de Estado, enquanto a inteligência militar fica a cargo de cada Força.

Compreendendo de forma mais completa a hierarquia do SISBIN, pode-se seguir para a análise mais prática do desenvolvimento da inteligência brasileira a partir das ações da ABIN e do gerenciamento do GSI/PR.

Zaverucha (2008) afirma que a lei que instituiu o SISBIN é de muitas formas ampla, sem possuir a definição do que seria o interesse nacional, que é por todo centrado nas ações desenvolvidas pelo Sistema, deixando tal conceituação a cargo daquele que ocupar a presidência da república, causando "uma ausência de definição sobre os limites de atuação e capacidade de operação da ABIN" (ZAVERUCHA, 2008, p. 181). Tal cenário, apesar de, em seu contexto, ser uma demonstração do baixo interesse do que estava se desenvolvendo na ABIN, mudou um ano depois da criação do Sistema, quando deu-se a instalação da Comissão Mista de Controle das Atividades de Inteligência (CCAI) que passou a gestar o controle do SISBIN (ZAVERUCHA, 2008). Contudo, apesar de suas deficiências de formulação, a instituição do SISBIN vem a integrar-se ao definido pela Política de Defesa Nacional (PDN) de 1996, onde dá-se, em sua sessão de Diretrizes: "n) aperfeiçoar a capacidade de comando, controle e inteligência de todos os órgãos envolvidos na defesa nacional, proporcionando-lhes condições que facilitem o processo decisório, na paz e em situações de conflito;" (BRASIL, 1996, p. 10).

A mudança de governo, de FHC para Lula, pouco alterou a instrumentalização do SISBIN (ZAVERUCHA, 2008), todavia, as alterações advindas dos novos documentos de Defesa, principalmente a Estratégia Nacional de Defesa (END), de 2008, trouxeram consigo, não uma reformulação, mas o estabelecimento mais claro das funções a serem desenvolvidas pela inteligência nacional (SILVA, 2014). A II PDN, publicada em 2005, veio apenas a ressaltar aquilo que já estava definido na versão de 1996, como uma manutenção do que deveria ser perseguido por uma Política de Defesa. Já a END denota que,

> Por meio da Inteligência, busca-se que todos os planejamentos – políticos, estratégicos, operacionais e táticos – e sua execução desenvolvam-se com base em dados que se transformam em conhecimentos confiáveis e oportunos. As informações precisas são condição essencial para o emprego adequado dos meios militares (BRASIL, 2012, p. 129).

A Estratégia também pontua que a Inteligência deve ser desenvolvida, de igual forma, em tempos de paz, já que "é da sua vertente prospectiva que procedem os melhores resultados, permitindo o delineamento dos cursos de ação possíveis e os seus desdobramentos" (BRASIL, 2012, p. 129), e, a exemplo disto, tem-se, junto ao GSI/PR, a Secretaria de Acompanhamento e Estudos Institucionais (SAEI), e o notável "Gabinete de Crises", criado em janeiro de 1999, "a quem caberia prevenir a ocorrência e articular o gerenciamento de crises" (COUTO, 2003, p. 3). O Gabinete é composto por membros das três Forças Armadas, do Itamaraty e da ABIN, que gerenciam o funcionamento das atividades de inteligência, objetivando a melhoria na

---

[10] O GSI/PR é órgão responsável pelo assessoramento direto da presidência em qualquer assunto relativo à defesa ou segurança nacionais, por apresentar ao Presidente a coordenação das atividades de inteligência, bem como a organização do gerenciamento de crises que atinjam de maneira demasiada a ordem pública (LIMA, 2012).

efetividade das ações, através da coordenação entre os órgãos que se utilizam das informações coletadas (COUTO, 2003).

Além disso, o documento também pontua as atividades de inteligência como uma das ações estratégicas que guiarão a implementação da END, que devem concretizar-se através do aperfeiçoamento do Sistema de Inteligência de Defesa, do devido aporte de recursos para seu funcionamento e aprimoramento, bem como, para uma contínua capacitação para análises nas áreas tecnológicas, cibernéticas, espacial e nuclear, sendo focadas, principalmente, nas atividades de monitoramento e controle (BRASIL, 2012).

De forma mais prática, cabe aqui o apontamento do desafio primordial do SISBIN. O Pan-Americano de 2007 foi o primeiro evento nacional de grandes proporções depois da formulação do SISBIN, logo, uma operação única foi montada para os jogos, congregando 25 órgãos públicos de segurança, das três esferas governamentais, canalizadas em "produzir conhecimentos de Inteligência para garantir a segurança do evento e das delegações esportivas" (ABIN, 2018e). Com o estabelecimento do Centro de Inteligência dos Jogos Pan-Americanos (CIJ), formou-se um modelo nacional de ação para grandes eventos, que voltou a ser utilizado na Conferência Rio+20 e na Copa do Mundo de 2014, e, de forma ainda mais relevante, serviu de catalisador de integração do SISBIN, aprofundando as relações entre os diferentes órgãos que serviram ao CIJ (ABIN, 2018f).

Em um segundo impacto mais palpável da atividade de inteligência, podemos citar a Operação Hileia Pátria, de 2013, que teve seu principal escopo no combate ao desmatamento na região amazônica. A ABIN atuou, através de um trabalho integrado, na análise, sistematização e difusão dos dados e informações produzidas pela própria agência e pelas outras instituições ligadas ao SISBIN, otimizando os resultados das ações realizadas nas áreas de desmatamento ilegal cobertas pela operação (ABIN, 2018g).

E, com um impacto mais amplo, as Operações Ágata, ocorridas entre os anos de 2011 e 2016, com o envolvimento de forças federais e estaduais, tiveram por objetivo combater aos atos ilícitos ocorridos em toda fronteira terrestre do Brasil, bem como, aumentar a presença do país nas regiões limítrofes. Através de Centros de Inteligência Regionais (CIR), instalados em todos os estados abrangidos pelas operações, a ABIN produziu conhecimentos que colaboraram na preparação das estratégias para a operação, antecipando obstáculos e dando auxílio às missões repressivas (ABIN, 2018i).

A hierarquia do SISBIN foi reformada no governo Dilma, em 2015, quando da reforma dos gabinetes, tendo a ABIN sendo transferida para a Secretaria de Governo, onde permaneceu até a chegada do presidente Michel Temer ao poder, quando retornou a égide do GSI/PR e onde está até o momento (ABIN, 2018c). Especialmente no governo Temer, houve três dos maiores avanços relativos ao funcionamento da atividade de Inteligência.

Primeiramente, a Política Nacional de Inteligência (PNI), onde se "estabelece diretrizes, limites e parâmetros à atuação da Inteligência federal, desenvolvida pela ABIN e por todos os órgãos integrantes do Sistema Brasileiro de Inteligência (SISBIN)." (ABIN, 2018h); em um segundo momento, e onde concentramos nossa atenção futura, a Estratégia Nacional de Inteligência (ENINT), aprovada pelo Decreto presidencial de 15 de dezembro de 2017, traz em seu bojo a primeira definição mais ampla dos conceitos adquiridos desde 1999, definindo a missão do SISBIN, como "desenvolver a Atividade de Inteligência, de forma integrada, para promover e defender os interesses do Estado e da sociedade brasileira." (BRASIL, 2017, p. 11); a visão, projetada pela "excelência e integração no desempenho da Atividade de Inteligência, tornando-a imprescindível para a garantia da segurança e dos interesses do Estado e da sociedade brasileira." (BRASIL, 2017, p. 11); e estando sempre amparada nos princípios éticos do respeito, da imparcialidade, da cooperação, da descrição, do senso crítico e pela excelência (BRASIL, 2017); e, mais recentemente o Plano Nacional de Inteligência (PLANINT), que, em

uníssono ao PNI e ao ENINT, monta o embasamento final ao desenvolvimento das atividades de inteligência (ABIN, 2018a).

Através da ENINT, o Brasil define pela primeira vez uma agenda de desafios a serem superados pela inteligência e de objetivos a serem alcançados, além de apontar os eixos que estruturarão esses processos (BRASIL, 2017), e que, com seu devido espaço, serão abordados, todavia, não estando somente relacionados a ENINT, mas a própria realidade das atividades de inteligência no Brasil.

3. DESAFIOS SECURITÁRIOS DO BRASIL COM RELAÇÃO À ESTRATÉGIA NACIONAL DE INTELIGÊNCIA E DEFESA

A formulação e divulgação da ENINT, conforme supracitado, é um ato recente diante do histórico do sistema nacional de inteligência. Segundo a ABIN, esse documento é basilar para o recém decretado Plano Nacional de Inteligência (ABIN, 2018a), e diante de tal fato, esta seção objetiva-se a analisar sua contribuição para a área de inteligência e defesa nacional a partir das ameaças, desafios e oportunidades nele observados, assim como, apresentar perspectivas atuais e futuras para a defesa da nação diante da importância e crescimento das atividades de inteligência. Não obstante e apesar de sua primazia, a presente análise não se limita apenas à ENINT, como também aborda outras contribuições bibliográficas, incluindo os alicerces nacionais da atividade de inteligência e defesa do Brasil.

3.1. A formulação e os objetivos estratégicos da ENINT

A Estratégia Nacional de Inteligência, colocada em vigência pelo governo de Michel Temer a partir do Decreto de 15 de dezembro de 2017, surge como um mecanismo de fortalecimento da atuação do SISBIN e da ABIN, através da qual ficam definidos os objetivos estratégicos atrelados às atividades de inteligência do Estado brasileiro, bem como, se estabelece a agenda de desafios relacionados aos setores de Defesa e Segurança, e as oportunidades que podem surgir para a expansão desta atividade no eixo securitário brasileiro.

A partir do documento que homologa a criação da ENINT, é possível verificar o histórico das atividades de inteligência no Brasil, bem como, o desenvolvimento da PNI e do SISBIN dentro do ambiente estratégico do Estado, e os princípios éticos que norteiam a sua formulação e funcionamento, para o alcance daqueles que são colocados como seus objetivos estratégicos principais.

Com relação a estes objetivos, o documento que valida a ENINT descreve, de forma clara e objetiva, os 33 objetivos estratégicos que irão conduzir a implementação da Atividade de Inteligência à Defesa e Segurança do Estado brasileiro, em um eixo temporal de 5 anos, ou seja, tratam-se de objetivos de curto prazo para a melhora na atuação do SISBIN.

No documento oficial não há uma ordem de importância para a apresentação destes objetivos, constando apenas uma divisão geral em quatro eixos estruturantes – i) Atuação em rede; ii) Tecnologia e Capacitação; iii) Projeção Internacional e iv) Segurança do Estado e da Sociedade – nos quais os mesmos são elencados. Entretanto, de modo a facilitar a compreensão destes objetivos e das áreas tangenciadas por eles, consideramos pertinente uma divisão mais minuciosa para o agrupamento desses itens. Assim, após analisar os Objetivos Estratégicos da Estratégia Nacional de Inteligência, optamos pela divisão em sete micro eixos (dentro dos eixos principais) de estruturação para o melhoramento do SISBIN, sendo elas:

<u>Eixo 1 - Atuação em Rede</u>

Aprimoramento de processos: engloba melhorias nos processos de comunicação e compartilhamento de informações, assim como no mapeamento e gerenciamento das ações do SISBIN, na definição de critérios para ação conjunta com outras organizações, na criação de

protocolos para salvaguarda das informações e para a gestão dos riscos que a atividade de inteligência assume ao lidar com dados sigilosos (BRASIL, 2017b);

Melhorias nas capacidades e infraestrutura para a coleta de dados: gira em torno da ampliação das capacidades do Estado na obtenção de dados por meio da inteligência cibernética, através do fortalecimento do potencial de pesquisa e desenvolvimento tecnológico nas áreas de informação e comunicação, e a modernização das atividades de compilação, segurança e lapidação de grandes volumes de dados, para uso nas mais diversas finalidades (BRASIL, 2017b).

Eixo 2 - Tecnologia e Capacitação

Aumento da qualificação e capacitação técnica para atuação nas atividades de inteligência: circunda o âmbito das melhorias na qualificação da mão-de-obra que irá desempenhar as atividades de inteligência junto aos órgãos vinculados aos SISBIN. Isso inclui a promoção da ampliação da oferta de cursos relacionados à área de Inteligência e exploração do campo cibernético, a estruturação de capacitações conjuntas entre agências voltadas a este domínio e o preparo dos agentes diplomáticos para exercício da função de expandir a representação da atividade de Inteligência brasileira no exterior (BRASIL, 2017b).

Eixo 3 - Projeção Internacional

Aumento das redes de conexão e intercâmbio de informações no âmbito internacional: este objetivo da ENINT demonstra o interesse em inserir o Brasil em fóruns, eventos e encontros internacionais como um polo de estudo e desenvolvimento da Inteligência, de modo a conseguir ampliar as redes de parcerias e acordos de cooperação internacional também para o âmbito da segurança e defesa dos Estados através das estratégias de inteligência. Ainda, foca também na expansão do apoio estatal às instituições em sua atuação na esfera internacional, ampliando as redes de intercâmbio informacional entre os diferentes órgãos brasileiros que dispõem de atuação no exterior (BRASIL, 2017b).

Eixo 4 - Segurança do Estado e da Sociedade

Aprimoramento dos conhecimentos e redes de compartilhamento de informação voltadas às principais ameaças reconhecidas pelo Estado: neste item, são apresentados os objetivos ligados diretamente às tarefas de defesa com relação às ameaças que o Estado toma como latentes, que se tratam de: i) Corrupção; ii) Crime Organizado; iii) Ilícitos Transnacionais; iv) Terrorismo. A fim de consolidar relevância a Estratégia Nacional de Inteligência na resolução destas questões, este agrupamento de objetivos foca no fomento à produção de conhecimentos técnicos sobre esta temática, assim como, no aprimoramento dos canais de veiculação de informações diretas sobre estas ameaças, de modo que possam ser mais rapidamente mitigadas, e por fim, concentra-se também na criação de novos protocolos específicos para a atuação integrada entre o SISBIN e demais Sistemas de Segurança (SisGAAZ, SisFron) para a formulação de estratégias de combate às ameaças à soberania estatal (BRASIL, 2017b).

Melhorias nos sistemas de alerta e protocolos de ações diversas: os objetivos enquadrados nesta seção permeiam o melhoramento das competências relacionadas à identificação dos principais interesses nacionais relacionados à defesa contra ações adversas, bem como, o estabelecimento de sistemas de alerta para prevenção e a criação de protocolos de atuação integrada para a neutralização de ações adversas (BRASIL, 2017b).

Melhoria do acompanhamento de processos legislativos que tangenciam as atividades de inteligência: esta última seção de objetivos atenta-se para o acompanhamento e apoio na condução dos processos decisórios que tangenciam o Poder Legislativo, de modo que as decisões e marcos legais sejam implementados com maior rapidez e eficácia, tornando a

atividade de inteligência em um dos maiores recursos estratégicos do Estado brasileiro (BRASIL, 2017b).

Dado o caráter não individual de tais objetivos, sendo prioridades também entre os Estados do continente sul-americano, faz-se indispensável a reflexão acerca do esforço de integração com o entorno estratégico brasileiro. A América do Sul trata-se de um continente que emerge com um histórico de autonomia bastante vulnerável, do qual surge a necessidade da orquestração de mecanismos capazes de fomentar a emancipação da região com relação ao norte global. Dentro deste propósito, a capacidade de conjugar ferramentas de uso comum que possam garantir maior margem de manobra quanto à tratativa das ameaças da região, pode ser a pedra basilar para o desenvolvimento da autonomia regional.

Sob ótica dos eixos estruturantes para o alcance dos objetivos da ENINT, algumas iniciativas já foram adotadas no âmbito regional, como forma de viabilizar os debates acerca do desenvolvimento conjunto, e estas poderiam funcionar como fios condutores entre os objetivos de cada Estado quanto ao alargamento de suas atividades de Inteligência e Segurança. A título de exemplo, temos a Iniciativa para a Integração da Infraestrutura Regional Sul-Americana (IIRSA), criada em 2000, que tem como foco o desenvolvimento infra estrutural básico nas áreas de transporte, comunicações e energia, disponibilizando as bases para uma maior integração comercial e social do subcontinente sul-americano (COUTO, 2006). Da mesma forma, há também a Escola Sul-Americana de Defesa (ESUDE), que surge como iniciativa entre os Estados Sul-americanos para criar uma maior convergência nos assuntos de caráter estratégico, a partir dos "[...] altos estudos, da construção de uma metodologia comum de medição dos gastos em defesa, um importante intercâmbio em matéria de formação e capacitação militar, entre outros pontos igualmente meritórios." (FUCCILLE, 2014, p. 9) a fim de atingir objetivos mútuos, passando pelo escopo infra estrutural tratado pela IIRSA.

Há ainda, a União das Nações Sul-Americanas (UNASUL) - que visa uma maior integração em todos os âmbitos, passando também pela questão securitária; o Conselho de Defesa Sul-Americano que tem por objetivo ser um mecanismo de conexão para o estabelecimento de políticas de defesa coletivas entre os países da região (FUCCILLE, 2014), e a Zona de Paz e Cooperação do Atlântico Sul (ZOPACAS) que em conjunto com outras dinâmicas regionais (nações latino americanas e africanas banhadas pelo Atlântico Sul) visa expandir suas redes de compartilhamento de informações, tendo em vista a elaboração de políticas de defesa e estabilidade no comando e utilização de espaços comuns, que sejam igualmente benéficas a todos os envolvidos.

Todas estas iniciativas poderiam ser vistas como palco, tanto para a discussão e coordenação de esforços para solucionar problemas comuns à região, quanto para o aperfeiçoamento dos processos que levam ao atingimento dos objetivos, não somente da ENINT, mas também os regionais. Todavia, ao entrar no cerne das atividades de Inteligência, circunda-se uma linha tênue que impõe limites, correlacionados à tramitação de informações de caráter sigiloso que estão diretamente ligados ao interesse estatal, criando barreiras à integração completa, pela exiguidade de uma consciência de segurança coletiva, que seja capaz de transcender o campo da Inteligência de Estado, para a possível criação de um campo de Inteligência Regional.

3.2. O que a agenda da ENINT classifica como ameaças

Em princípio, a necessidade de avaliação das possíveis ameaças se faz indispensável em um contexto em que sua análise toma posição prioritária para a segurança do país diante de ações que possam vir a causar danos à nação, sendo que tais empreendimentos podem ser oriundos tanto de fatores ou atores externos quanto internos (BRASIL, 2017b). Diante disso, a ENINT classifica como ameaças onze itens, a maioria dos quais buscaremos abordar ao longo dessa seção, iniciando pelos ataques cibernéticos, uma nova e crescente ameaça.

O documento caracteriza como ataques cibernéticos qualquer ação deliberada que empregue recursos da tecnologia da informação com o intuito de "interromper, penetrar, adulterar ou destruir redes utilizadas por setores públicos e privados" (BRASIL, 2017b, p. 17) cuja essência é fundamental para a sociedade civil e para o Estado, com destaque para a infraestrutura crítica nacional (BRASIL, 2017b). Entendemos como infraestruturas críticas "as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional" (BRASIL, 2010).

A manutenção e preservação dessas áreas são fundamentais para o Estado, e um exemplo das consequências de falhas na proteção de tais infraestruturas pode ser observado no recente caso de um dos maiores ataques cibernéticos da história, perpetuado em 2017 por um grupo de hackers que obtiveram uma "arma cibernética" roubada da Agência Nacional de Segurança dos EUA (NSA) e "sequestraram" a computadores em 150 países em troca de um resgate financeiro através do *ransomware* WannaCry. O ataque atingiu diversas infraestruturas críticas ao redor do mundo, como o Serviço Nacional de Saúde britânico (*National Health Service* - NHS, tradução própria) e o Ministério do Interior russo (GRAHAM, 2017).

A PNI também atribui o caráter de ataque cibernético à manipulação de opiniões através da propaganda ou desinformação (BRASIL, 2016), uma forma de ataque que os Estados Unidos acusam a Rússia de ter perpetuado através de perfis falsos nas redes sociais (inclusive com alguns utilizando fotos de cidadãos brasileiros alheios ao ocorrido) em suas mais recentes eleições presidenciais, uma infraestrutura nacional basilar em governos democráticos (WHITAKER, 2018; SHANE, 2017). Diante de tal ameaça, a ENINT classifica como oportunidade o desenvolvimento científico e tecnológico e o emprego de inteligência cibernética para que o Brasil possua maior capacidade de frustrar futuros ataques, assim como para posicionar o país em um patamar mais competitivo no cenário internacional (BRASIL, 2017b).

Em conformidade com a ENINT, a Política Nacional de Defesa destaca, no que tange o ambiente internacional e as oportunidades e ameaças referenciadas, que:

> Os avanços da tecnologia da informação, a utilização de satélites, o sensoriamento eletrônico e outros aperfeiçoamentos tecnológicos trouxeram maior eficiência aos sistemas administrativos e militares, sobretudo nos países que dedicam maiores recursos financeiros à Defesa. Em consequência, criaram-se vulnerabilidades que poderão ser exploradas, com o objetivo de inviabilizar o uso dos nossos sistemas ou facilitar a interferência à distância. Para superar essas vulnerabilidades, é essencial o investimento do Estado em setores de tecnologia avançada (BRASIL, 2012, p. 19).

Nota-se que o governo brasileiro faz referência à capacidade de interferência externa contra a soberania e os interesses nacionais, especificamente através de meios digitais, mas que essencial e geralmente se manifestam como atos perpetuados por outros Estados ou atores que buscam intervir na política nacional guiados pelos seus próprios objetivos em detrimento dos objetivos nacionais (BRASIL, 2017b).

A ENINT propõe o combate a possíveis ingerências exteriores através do fortalecimento cultural de proteção e discrição ao conhecimento sensível, tal qual as fontes, agentes e ativos que devem ser preservados em compromisso com a boa performance da atividade de inteligência brasileira (BRASIL, 2017b). Em relação a isso, o Livro Branco de Defesa Nacional atribui ao Sistema de Inteligência de Defesa (SINDE) a tarefa e responsabilidade de "salvaguardar conhecimentos do interesse da Defesa" fomentando a interação entre as etapas de planejamento e execução do processo decisório estratégico nacional (BRASIL, 2012, p. 77).

Garantidos esses compromissos, mediante a atual conjuntura nacional, a delimitação da corrupção como ameaça à atividade de inteligência e aplicação da estratégia nacional é

bastante atual e importante em conformidade com o interesse nacional, visto que a deturpação da atividade política produz o descrédito das instituições estatais e, por conseguinte, a perda de apoio popular e a desconexão entre as autoridades governamentais e a sociedade civil (BRASIL, 2017b).

Diante da apresentação da corrupção como um obstáculo para a atividade de inteligência brasileira e a defesa nacional, o país propõe o enfrentamento a esse fator em conjunto com os demais fatores considerados e classificados no Livro Branco de Defesa, tal qual na ENINT, como "ilícitos transnacionais", dentre os quais se encontram também o terrorismo, o tráfico de pessoas, armas e narcóticos e o crime organizado. Diante desses ilícitos, o Brasil deve buscar estabelecer, conforme proposto na ENINT (2017, p. 23), "soluções conjuntas, com a participação de diferentes atores governamentais" condicionando o êxito no combate a tais ameaças com a produção e proteção de conhecimentos importantes e necessários para tal enfrentamento, assim como a interação e cooperação entre as agências e entidades nacionais e governos e organizações externas (BRASIL, 2017b). No que tange a cooperação com entidades externas, destacamos a importância de nos atermos ao entorno estratégico, conforme exposto em nossa Política de Defesa Nacional, em prol da redução da probabilidade de conflitos, priorizando a cooperação regional no âmbito da América do Sul através de organizações como o Mercosul, a UNASUL e a Organização do Tratado de Cooperação Amazônica; e no âmbito da Zona de Paz e Cooperação no Atlântico Sul para a proteção de nossos interesses e segurança marítimos e costeiros (MOREIRA, 2011), porém, através de uma ótica realista, bastante cautelosos ao perigo de espionagem.

A Espionagem, segundo a ABIN, é uma ação realizada por um agente que busca, clandestinamente, lograr acesso a informações sigilosas ou sensíveis de um determinado governo ou de instituições nacionais em benefício de outros países, organizações, grupos, entre outros (ABIN, 2018b). Pode ser realizada na forma cibernética, conforme os ataques já aqui mencionados.

Este tipo de atividade pode trazer um enorme prejuízo para um país, no âmbito econômico, no que se refere a competitividade com outros países ou empresas, bem como na área de segurança e estratégia, pois acessa informações que não estariam livremente disponíveis e expõem as decisões de um país, sua política externa, domínio de tecnologias avançadas, questões militares e científicas. A ABIN realiza um trabalho no sentido de detectar e neutralizar esse tipo de ameaça (BRASIL, 2017b). Outra forte ameaça que podemos referir é a Sabotagem, definida n ENINT como:

> uma ação deliberada, com efeitos físicos, materiais ou psicológicos para destruir, danificar, comprometer ou inutilizar, total ou parcialmente, definitiva ou temporariamente, dados ou conhecimentos; ferramentas; materiais; matérias-primas; equipamentos; cadeias produtivas; instalações ou sistemas logísticos, sobretudo aqueles necessários ao funcionamento da infraestrutura crítica do país (BRASIL, 2017b, p. 17).

Atualmente no Brasil, o foco da defesa de sabotagem está voltado para a agricultura que se vê ameaçada por agentes químico-biológicos, o que pode provocar um imenso impacto na economia e na segurança do país. Nessa mesma linha, o país está se voltando também para a defesa contra o agroterrorismo, que seria a introdução proposital de organismos como vírus, fungos, insetos ou bactérias para prejudicar culturas, podendo trazer prejuízos à saúde, ao meio ambiente e à economia, no sentido de fazer o país perder seu lugar como exportador desta cultura (MONTENEGRO, 2005).

A legislação brasileira assim define Terrorismo no artigo 2º da Lei n º 13.260/2016: “consiste na prática por um ou mais indivíduos dos atos previstos neste artigo, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com

a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública” (BRASIL, Lei nº 13260/2016).

O Terrorismo representa uma grave ameaça à paz e à segurança dos Estados. O Brasil não é considerado um alvo específico de grupos terroristas, no entanto, não está livre de eventuais episódios, tampouco de efeitos decorrentes de ataques terroristas, que podem ser sociais, políticos, econômicos (ABIN, 2018j). Este assunto é acompanhado pela inteligência em âmbito mundial (BRASIL, 2017b). Uma das formas de atuação que o Brasil usa contra o terrorismo é a troca de informações com serviços de inteligência estrangeiros (ABIN, 2018j).

Armas de destruição em massa, constituem uma forte ameaça no sentido de que uma única utilização pode causar um elevado dano, número excessivo de mortes. Representa risco à paz mundial e principalmente aos países que abdicaram do uso destas armas (BRASIL, 2017b). O Brasil assinou o Decreto nº 8.669 de 2016 reafirmando compromisso contra esse tipo de ameaça. O decreto obriga todas as autoridades brasileiras, "no âmbito de suas respectivas atribuições", a cumprirem as resoluções 1540, de 2004, e 1977, de 2011, ambas adotadas pelo Conselho de Segurança da Organização das Nações Unidas (ONU), embora o Brasil já adotasse medidas nesse sentido.

A Criminalidade organizada, ameaça a segurança de todos os Estados e de suas populações, e sua incidência, notadamente em sua vertente transnacional, reforça a necessidade de aprofundar a cooperação (BRASIL, 2017b). Diagnosticar organizações criminosas que ameaçam o território brasileiro é atividade relevante na estratégia e no processo de tomada de decisão do Governo Nacional. Esses aspectos são de atribuição da Inteligência de Estado, que por meio de informações permite antecipar e mitigar os riscos, bem como solucionar eventuais vulnerabilidades detectadas (BRASIL, 2017b).

3.3. Os desafios da Inteligência Nacional

A Inteligência, como uma atividade de segurança e defesa, tem em seus desafios o centro de sua operacionalidade e de sua realidade, corrente e vindoura, pois estes demonstram todas áreas as quais os tomadores de decisão devem concentrar sua atenção. Com o objetivo de identificar estes fatos, a ENINT pontua dez desafios à consecução da inteligência nacional, que serão discorridos a seguir:

I - Fortalecimento da atuação integrada e coordenada da Atividade de Inteligência – A essencialidade da integração entre todas as partes do SISBIN e, por ventura, das forças de segurança, já encontrou respaldo na realidade, ao caso da coordenação ocorrida com a ABIN durante os Jogos Olímpicos e Paraolímpicos de 2016, que, em consonância com o setor de Segurança, sob gerência da Casa Civil da PR, manteve durante 60 dias, 24h, mais de 400 agentes em atividade, garantido a produção e a divulgação de informações necessárias à manutenção da segurança do evento (BRASIL, 2017b; ABIN, 2018f).

II - Fortalecimento de cultura de proteção do conhecimento e de preservação do sigilo – Perpassando a atividade inteligência e alcançando todos os meios sociais, o incentivo a uma cultura de proteção aos conhecimentos e agentes sensíveis à segurança nacional, torna-se parte da inteligência, ao passo que dificultam e impedem as interferências externas, não vindo a comprometer o interesse nacional (BRASIL, 2017b).

III - Ampliação e aperfeiçoamento do processo de capacitação para atuação na área de Inteligência – O SISBIN é mantido pelo trabalho de agentes, especializados em suas mais diversas áreas, todavia, principalmente na área tecnológica, onde os avanços são sempre rápidos, o contínuo aprimoramento é necessário para que se dê uma resposta adequada a qualquer ameaça a defesa nacional, para tanto, é preciso o investimento, capacitação e

atualização constante dos servidores que asseguram o funcionamento das atividades de inteligência (BRASIL, 2017b).

IV - Maior utilização de tecnologia de ponta, especialmente no campo cibernético – Como mencionado no item anterior, a área de tecnológica, bem como a cibernética, são as de maiores avanços, tanto em aprimoramento quanto em uso. Logo, fazer-se uma constante atualização dos equipamentos, segue como um desafio a toda a Atividade de Inteligência, tanto em sua ação ativa quanto defensiva (BRASIL, 2017b).

V - Intensificação do uso de tecnologias de tratamento e análise de grandes volumes de dados (*Big data e Analytics*) – A era da informação trouxe consigo um crescimento exponencial das informações disponíveis na rede. Redes sociais, bancos de dados e bibliotecas digitais formam enormes arquivos, que, entre as informações ali contidas, podem estar contidas ameaças ou informações chave a segurança nacional. Fazer-se uso de ferramentas que permitam analisar essas grandes quantidades de dados permitirá aos agentes produzirem conhecimentos com resultados potenciais e reais mais eficazes e, em um caso da necessidade da ação do Estado brasileiro, a reconhecer a captura de dados, como a exemplo, as recentes denúncias da utilização dessas fontes de dados para a manipulação e direcionamento de informações durante as eleições de 2014, o que pode ou poderia, contribuir para a manipulação de resultados (BRASIL, 2017b; BRIGATTO, 2018).

VI - Ampliação da internacionalização da Atividade de Inteligência brasileira - O amadurecimento e integração possibilita a projeção da atividade de Segurança e Defesa brasileira, tivemos através do papel da ABIN na Rio+20 uma perfeita projeção de inteligência, abrangendo na organização de toda a inteligência a nível federal e regional, amplamente elogiado e reconhecido pela Organização das Nações Unidas (ONU) (BRASIL, 2017b).

VII - Apoio ao fortalecimento da inserção do país no cenário internacional - Tivemos através da ABIN um fortalecimento de nossas fronteiras que compreende aproximadamente 150 km dos limites de todo o território nacional, tal feito de grande dificuldade devido sua tamanha extensão propicia ao Estado brasileiro uma excelente ferramenta de projeção da sua defesa e estratégia em conjunto com seus países vizinhos para a proteção de suas respectivas soberanias, colaborando para a projeção de nossas políticas de inteligência e defesa nacional inseridas no contexto globalizado e dinâmico atual. Desafio de extrema complexidade pois envolve o crime organizado, o tráfico de armamento e contrabando bélico e inserção de drogas em todo o território (BRASIL, 2017b).

VIII - Apoio ao combate à corrupção, ao crime organizado, aos ilícitos transnacionais e ao terrorismo - Temos também como ferramenta de defesa nacional a inteligência responsável por administrar e aplicar sistemas de defesa que coíbam a corrupção sistêmica que ocorre em nosso solo nacional, através da ABIN no qual integra a Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA). Sendo assim, os relatórios da ABIN auxiliam governo na prevenção à lavagem de dinheiro e corrupção. O crime organizado, perfeitamente englobado nesse contexto, dificulta e se transforma em um desafio constante e de complexa resolução. Temos na Copa do Mundo da FIFA de 2014, um ótimo exemplo da estratégia inteligente desenvolvida pela ABIN, fato este que possibilitou inúmeros planos de contingência a possíveis ataques terroristas em solo Brasileiro. (BRASIL, 2017b).

IX - Monitoramento e enfrentamento eficaz de ações adversas contra interesses nacionais - Temos através do sistema de Inteligência e Contra inteligência o diferencial em questões adversas ao interesse nacional, tendo na Contra inteligência a responsabilidade estratégica de

desenvolver ações voltadas para a prevenção, detecção e obstrução de possíveis ameaças aos interesses nacionais (BRASIL, 2017b).

X - Aprimoramento da legislação para a Atividade de Inteligência - Fica clara a atuação da ABIN em desenvolver novas políticas que contribuam para a segurança da inteligência nacional através dos constantes fluxos migratórios e os seus respectivos impactos políticos, sociais e econômicos para o Brasil. A Inteligência auxilia e subsidia a elaboração de novas políticas públicas que possibilitem e assegurem o acesso de novos imigrantes e refugiados ao país, garantindo que através destes fluxos migratórios o acesso seja feito de forma legal e que não ameacem a segurança de toda a sociedade brasileira (BRASIL, 2017b).

CONCLUSÃO

Tendo em vista os aspectos observados ao longo deste trabalho, e objetivando compreender o desenvolvimento das Atividades de Inteligência em um plano internacional, e, de maneira mais central, no Brasil, temos por fato a centralidade dessas atividades nas formulação, consecução e inserção das políticas de Segurança e Defesa de qualquer Estado. Sua referência central, como acompanhamos nos desenvolvimentos históricos e teóricos aqui observados, advém, principalmente, de sua essencialidade na formulação de estratégias, através da obtenção das melhores informações, que não estão somente ligadas às áreas legítimas dos castrenses, mas, de igual forma, nas diversas tonalidades do interesse estatal.

Em caso especificamente brasileiro, as Atividades de Inteligência, apesar de seu desenvolvimento tardio, têm apresentado uma espiral de crescimento ascendente em sua complexificação desde a criação do SISBIN, em 1999, e que foi coroada recentemente com o tripé formado pelo PNI, ENINT e PLANINT, que, dentro de um entendimento maior, demonstram o interesse do país em estar preparado em suas normas para desenvolver a Atividade de Inteligência e a responder a qualquer desafio proposto. Estes pontos convergem, primeiramente, com toda nova racionalidade e com o novo contexto impostos ao fim da Guerra Fria, no qual a partir da emergência de novos atores, da mudança de paradigmas geopolíticos e de parte do próprio contexto interno, fez-se necessária uma resposta adequada aos desafios ainda desconhecidos; e, em segundo momento, com o crescimento constante das tensões em nível internacional, da participação civil nos discursos securitários e da necessidade de uma reação aos desafios a segurança interna do país, torna-se primordial uma base sólida e moderna para a atuação dos órgãos de inteligência, dando embasamento ao seu trabalho.

Por fim, ao focar no que é apresentado pela ENINT, cabe aqui a deferência a imprescindibilidade de que o progresso normativo das Atividades de Inteligência seja devidamente acompanhado pelo progresso ímpar da área prática e estruturante da Inteligência nacional. O reavivamento e surgimento de diversas tensões ao redor do globo, a exigência pública interna de uma proteção estatal mais eficiente e da inserção do próprio interesse nacional perpassam não somente pelos referenciais teóricos e pelo delineamento de políticas, que são sim importantes em sua própria forma, mas que cairão por terra se não tiverem suas palavras transferidas para a realidade.

REFERÊNCIAS BIBLIOGRÁFICAS

ABIN = AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Decreto fixa a Política Nacional de Inteligência**. 2018a. Disponível em: <http://www.abin.gov.br/decreto-fixa-a-politica-nacional-de-inteligencia/>. Acesso em: 29 abr.2018.

______. **Espionagem**. 2018b. Disponível em: http://www.abin.gov.br/atuacao/fontes-de-ameacas/espionagem/>. Acesso em: 21 mar. 2018.

______. **Histórico**. 2018c. Disponível em: <http://www.abin.gov.br/institucional/historico/>. Acesso em: 21 mar. 2018.

______. **Inteligência e Contrainteligência**. 2018d. Disponível em: <http:// http://www.abin.gov.br/atividadeinteligencia/inteligenciaecontrainteligencia//>. Acesso em: 20 mar. 2018.

_______. **Jogos Pan-Americanos 2007**. 2018e. Disponível em: <http://www.abin.gov.br/grandes-eventos/jogos-pan-americanos/>. Acesso em: 21 mar. 2018.

______. **Jogos Olímpicos e Paralímpicos 2016**. 2018f. Disponível em: <http://www.abin.gov.br/grandes-eventos/olimpiadas-rio-2016/>. Acesso em: 21 mar. 2018.

_______. **Operação Hileia Pátria 2013**. 2018g. Disponível em: < http://www.abin.gov.br/atuacao/areas-prioritarias/meio-ambiente/operacoes-soberania-e-hileia-patria/>. Acesso em: 21 mar. 2018.

_______. **Plano Nacional de Inteligência é assinado**. 2018h. Disponível em: <http://www.abin.gov.br/plano-nacional-de-inteligencia-e-assinado-3/>. Acesso em: 06 mai. 2018.

_______. **Segurança das Fronteiras**. 2018i. Disponível em: <http://www.abin.gov.br/atuacao/areas-prioritarias/seguranca-das-fronteiras/>. Acesso em: 21 mar. 2018.

_______. **Terrorismo**. 2018j. Disponível em: <http://www.abin.gov.br/atuacao/fontes-de-ameacas/terrorismo/>. Acesso em: 21 mar. 2018.

ARAÚJO, Raimundo Teixeira de. **História Secreta dos Serviços de Inteligência: origens, evolução e institucionalização**. São Luís: Editora do autor, 2004. In: REVISTA BRASILEIRA DE INTELIGÊNCIA. Brasília: Abin, v.1, n.1, dez. 2005.

BRASIL. **Decreto 8.793, de 29 de junho de 2016**. Brasília DF, 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm>. Acesso em 29 abr. 2018.

______. **Decreto de 15 de dezembro de 2017**. Brasília, DF, 2017a. Disponível em: <http://www.abin.gov.br/conteudo/uploads/2015/05/ENINT.pdf>. Acesso em: 22 mar. 2018.

______. **Estratégia Nacional de Inteligência**. Brasília, DF, 2017b. Disponível em: <http://www.abin.gov.br/inteligencia-passa-a-contar-com-estrategia-nacional/>. Acesso em 22 mar. 2018.

______. **Guia de Referência para a Segurança das Infraestruturas Críticas da Informação**. Brasília, DF, 2010. Disponível em: <http://dsic.planalto.gov.br/legislacao/2_Guia_SICI.pdf>. Acesso em: 20 mar. 2018.

______. **Lei Nº 9.883, de 7 de dezembro de 1999**. Brasília, DF, 1999. Disponível em: < http://www.planalto.gov.br/ccivil_03/Leis/L9883.htm>. Acesso em: 20 mar. 2018.

______. **Medida Provisória Nº 2.216-37, de 31 de agosto de 2001**. Brasília, DF, 2001. Disponível em: < http://www.planalto.gov.br/ccivil_03/MPV/2216-37.htm#art11>. Acesso em: 21 mar. 2018.

______. **Política Nacional de Defesa**. Brasília: Presidência da República, 1996. Disponível em:<http://www.biblioteca.presidencia.gov.br/publicacoes-oficiais/catalogo/fhc/politica-de-defesa-nacional-1996.pdf> Acesso em: 20 mar. 2018

______. **Política Nacional de Defesa & Estratégia Nacional de Defesa**. Brasília: Ministério da Defesa, 2012.

BRIGATTO, Gustavo. Facebook compartilhou com Cambridge Analytics 443 mil contas do Brasil. **Valor Econômico**, São Paulo, 5 abr. 2018. Disponível em: http://www.valor.com.br/empresas/5432807/facebook-compartilhou-com-cambridge-analytica-443-mil-contas-do-brasil>. Acesso em: 30 abr. 2018.

CEPIK, Marco. **Espionagem e democracia: Agilidade e transparência como dilemas na institucionalização de serviços de inteligência**. 1 ed. Rio de Janeiro: Editora FGV, 2003a.

______, Marco. **Sistemas nacionais de inteligência: origens, lógica de expansão e configuração atual**. Dados, Rio de Janeiro, v. 46, n. 1, p. 75-127, 2003b. Disponível em: < http://www.scielo.br/scielo.php?script=sci_arttext&pid=S001152582003000100003&lng=en &nrm=iso>. Acesso em: 20 mar. 2018.

COUTO, José Alberto Cunha Couto. O Gabinete de Segurança Institucional o gerenciamento de crises. In: **VIII Congresso Internacional do CLAD sobre a Reforma do Estado e da Administração Pública**, out. 2003, Panamá. Disponível em: <http://siare.clad.org/siare/biblo/biblo_a.html>. Acesso em: 21 mar. 2018.

COUTO, Leandro Freitas. A Iniciativa para a Integração da Infra-estrutura Regional Sul-americana – IIRSA como instrumento da política exterior do Brasil para a América do Sul. **Oikos**, Rio de Janeiro, v. 5, n. 1, jan. /dez. 2006.

DUROSELLE, Jean-Baptiste. **Todo império perecerá**: Teoria das relações internacionais. Brasília: Edunb, 2000.

EDWARD Snowden cita grampo de Dilma no Twitter. **G1**, 17 março 2016. Disponível em:<http://g1.globo.com/mundo/noticia/2016/03/edward-snowden-cita-grampo-de-dilma-no-twitter.html>. Acesso em: 25 abr. 2018.

FUCCILLE, Alexandre. Conselho de Defesa Sul-AMericano (CDS): Balanço e perspectivas. In: **IX Encontro da Associação Brasileira de Ciência Política**, Brasília, ago. 2014. Disponível em: <https://cienciapolitica.org.br/system/files/documentos/eventos/2017/04/conselho-defesa-sul-americano-cds-balanco-e-perspectivas-714.pdf>. Acesso em: 09 mai. 2018.

GILPIN, Robert. **War & Change in World Politics**. New York: Cambridge University Press, 1981. 288 p.

GONÇALVES, Joanisval Brito. A Atividade de Inteligência no Combate ao Crime Organizado: o Caso do Brasil. In: **REDES**, Santiago, out. 2003. Disponível em: <http://www2.senado.leg.br/bdsf/bitstream/handle/id/103/01.pdf?sequence=3>. Acesso em: 11 abr. 2018.

GRAHAM, Chris. NHS Cyber Attack: Everything you need to know about the 'biggest ransomware' offensive in history. **The Telegraph**. 20 maio. 2017. Disponível em: <https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/>. Acesso em: 24 abr. 2018.

LIMA, Mariana Fonseca. Percepções sobre a interação entre defesa, diplomacia e inteligência no Brasil. 2012. **Dissertação**, Mestrado em Relações Internacionais – Instituto de Relações Internacionais, Universidade de Brasília, Brasília. Disponível em: <

http://repositorio.unb.br/bitstream/10482/11615/1/2012_MarianaFonsecaLima.pdf>. Acesso em: 20 mar. 2018.

MAQUIAVEL, Nicolau. **O Príncipe**. 1998 ed. São Paulo: L&PM Pocket, 1998. 176 p.

MONTENEGRO, Mônica. Especial - Agroterrorismo: uma ameaça invisível a olho nu que começa a preocupar autoridades. **Câmara dos Deputados: Rádio Câmara**. 23 out. 2005. Disponível em: <http://www2.camara.leg.br/camaranoticias/radio/materias/REPORTAGEM-ESPECIAL/332242-ESPECIAL--AGROTERRORISMO:-UMA-AMEA%C3%87A-INVIS%C3%8DVEL-A-OLHO-NU-QUE-COME%C3%87A-A-PREOCUPAR-AUTORIDADES--(-4'-00%22-).html>. Acesso em: 11 mai. 2018.

MOREIRA, César Antônio Ciuffo. A atuação da Agência Brasileira de Inteligência no campo das relações internacionais brasileiras. 2011. **Monografia**, Especialização em Relações Internacionais – IREL, Universidade de Brasília, Brasília. Disponível em: <http://bdm.unb.br/handle/10483/2424>. Acesso em: 20 mar. 2018.

RIBEIRO, Fábio Pereira. Cooperação Estratégica em inteligência formação da defesa regional: uma contribuição dos serviços de inteligência. In: **Cadernos PROLAM/USP**, [S.l.], v. 5, n. 8, p. 113-128, junho 2006. Disponível em: <https://www.revistas.usp.br/prolam/article/view/81802>. Acesso em: 20 mar. 2018.

SEITENFUS, Ricardo. **Novos paradigmas da segurança coletiva internacional**. Santa Maria: Universidade Federal de Santa Maria, jan. 2003. Disponível em: <http://www.seitenfus.com.br/arquivos/novos-paradigmas.pdf>. Acesso em: 11 abr. 2018.

SHANE, Scott. The Fake Americans Russia Created to Influence the Election. **The New York Times**. 7 set. 2017. Disponível em: <https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html> Acesso em: 29 abr. 2018

SILVA, André Reis da. Segurança e Desenvolvimento da Projeção Internacional do Brasil (2003-2013). In: ARTURI, Carlos Schmidt (Org.). **Políticas de Defesa, Inteligência e Segurança**. Porto Alegre: UFRGS/CEGOV, 2014.

SENATOR Shelby speaks at the Heritage Foundation on intelligence and espionage in the 21st century. **Richard Shelby**. 09 mai. 2001. Disponível em: <https://www.shelby.senate.gov/public/index.cfm/floor-statements?ID=D05EE4D0-6D34-4A69-8998-BE0A971BCD6E>. Acesso em: 29 abr. 2018.

WHITAKER, Bill. When Russian Hackers Targeted the U.S. Elections Infrastructure. **CBS News**. 8 abr. 2018. Disponível em: <https://www.cbsnews.com/news/when-russian-hackers-targeted-the-u-s-election-infrastructure/>. Acesso em: 29 abr. 2018.

ZAVERUCHA, Jorge. De FHC a Lula: a militarização da Agência Brasileira de Inteligência. In: **Rev. Sociol. Polit.**, Curitiba, v. 16, n. 31, p. 177-195, nov., 2008. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S010444782008000200013&lng=en&nrm=iso>. Acesso em: 20 abr. 2018.